PMW 161 INFORMATION ASSURANCE

INFORMATION ASSURANCE (IA)
TECHNICAL AND MANAGEMENT SUPPORT

STATEMENT OF OBJECTIVES (SOO)

05 January 2004

1.0 SCOPE, BACKGROUND AND INTRODUCTION

1.1 SCOPE

This Statement of Objectives (SOO) prescribes the requirements for security systems engineering and the technical and program management in support of the Navy and DoD Information Assurance (IA) projects and IA initiatives assigned to the Information Security Systems Program (ISSP) Program Management Office, PMW C161.

1.2 BACKGROUND

The secure movement of information is vital to the well being of the nation and thus, critical to its peacekeeping and warfighting elements. Every aspect of naval operations from planning to deployment to the prosecution of war is supported and advanced by a complex information infrastructure. When our information is superior, the United States enjoys the advantage of information dominance. The concept of information dominance reflects the United States' awareness and understanding of the importance of that information infrastructure.

The discipline that leads to the achievement of this information dominance is described as Information Assurance (IA). IA has three primary elements: IA Defend; IA Attack; and IA Exploit, which combine to provide our naval warfighters with information dominance. These IA elements ensure the continued availability, confidentiality, and integrity of information while simultaneously denying those features to the adversary. The three elements work in concert to produce the following holistic IA capability:

(a) Information Defense to protect, detect, and react;
(b) Information Attack to disrupt the adversary's Command, Control, Communications, Computers, and Intelligence (C^4I) capabilities;
(c) Information Exploit to take advantage of the adversary's C^4I capabilities and weaknesses

The IA element assures the integrity, availability, and confidentiality of the information used by our Naval forces. Therefore, defending all information (e.g., data, voice, video, & imagery) and the information/communication systems and resources that process it must be protected from adversarial exploitation. As such, IA broadly encompasses information systems security (INFOSEC), TEMPEST, NMCI, and physical security mechanisms.

1.3 INTRODUCTION

The Program Executive Office (PEO) C4I & Space and SPAWAR are responsible for all aspects of the acquisition, fielding and support of Networks and Information Assurance systems within the Department of the Navy (DoN). The Information Security Systems Program Office (PMW C161) is an integral component within the PEO and SPAWAR, and is responsible for acquisition functions to develop, acquire or procure, field and support information security system products and services to meet valid Naval requirements. In addition, PMW C161 is tasked as the IA Technical Authority within the DoN and has the responsibility to supervise and approve all technical aspects of Naval Information Assurance. PMW C161 is also the Navy's Certification Authority and provides a wide range of system security engineering expertise and services to help adequately secure and operate the Department of Navy's (DoN's) infrastructures, systems, and applications.

1.3.1 THE ISSP PROGRAM MANAGEMENT OFFICE (PMW C161)

PMW C161 is responsible for providing Information Assurance, Defensive Information Operations, and Information Systems Security solutions and support to the Department of the Navy (including Marine Corps), and the Coast Guard's operational and acquisition organizations.

PMW C161 is responsible for all planning and execution of IA research, development and acquisition; fielding; integration; installation; test; support (throughout the life cycle); vulnerability, risk, and threat assessment; certification & accreditation; and security design and oversight for development programs—while incorporating the lessons learned into Navy education, training and awareness efforts.

The mission for the Information Security System Program Office is to:

(a) Serve as technical lead for Navy IA
(b) Provide systems security engineering and integration support for all DoN Information Systems with IA requirements
(c) Develop and manage DoN IA Research and Development (R&D) programs
(d) Budget for DoN IA programs
(e) Develop and acquire standard and specified IA products (Various Crypto devices/components, Various types of Secure Telephone Equipment, Host/Network Intrusion Detection Systems, Embedded Firewalls, Enclave Boundary Protection systems, Intelligent Agent Security Modules, Virtual Private Networks, Public Key Infrastructure card readers/tokens, Electronic Key Management devices and Cross Domain Solutions.

The IA program is currently focused on Mission Capabilities Team (MCT) initiatives that will be addressed within the scope of the SOO. A Mission Capability is described as:

(a) A specific operational ability or set of abilities (endorsed by OPNAV N614 and Validated Through IA ESG) required by fleet units to fulfill operational missions
(b) An operation that directly addresses one or more of the IA objectives as set forth by the IA ESG and described in section 3.5.

The following items (1-7) listed below are major Mission Capability Team initiatives for which PMW-C161, as the IA acquisition agent for the Navy, is responsible for the procurement, integration and sustainment of products, services and technologies. For a description of these initiatives see section 3.5 of this SOO.

1. Network Security Systems (NSS)
2. Navy Cryptographic (Readiness and Modernization)
3. Information Assurance (IA) Readiness
4. Secure Voice (SV) Communications
5. Multiple Security Level (MSL)
6. Key Management Infrastructure (KMI)
7. Security Systems Engineering for Emerging Fleet Initiatives (SSE)

This Statement of Objectives (SOO) addresses the technical security systems engineering and technical security system program management support services required by PMW C161 and other organizations within the PEO (C4I and Space) and SPAWAR and Director Navy, Marine Corp Intranet (NMCI) to effectively and efficiently fulfill their missions. The technical security engineering and program management support provided by the contractor shall ensure the timely and successful implementation of IA products/services across DoN C4ISR systems. The scope of the support will span both Commercial Off the Shelf (COTS) and Government Off the Shelf (GOTS) development and implementation as well as the development of policies/procedures for Information Assurance/Information Operations (IA/IO) systems. The scope of technical support requirements within this SOO will include but is not limited to the following areas: security systems engineering, implementation/installation support, software engineering, systems engineering, integrated logistics support, and program management. Services will be performed at fixed sites and mobile platforms in both U.S. and occasionally, non-U.S. locations.

Implementation of these engineering services and program management support will be accomplished by a single award Performance-Based Acquisition Services (PBSC) contract that will focus on program management, security systems engineering and technical assistance IA development, production and implementation of Information Security Systems. The tasks generated throughout the period of performance of this contract will address program management, INFOSEC techniques, analysis of security system architecture, design for equipment and systems, and the life cycle support required for IA system design and equipment development, procurement and implementation.

For this contract vehicle, services shall be accomplished through the execution of written Task Orders (TOs) to be delivered to the program office (PMW C161). Individual TOs will utilize Performance Based methodology to the maximum extent possible. The TO will, at a minimum, provide a description of the effort to be performed, labor cost/hours, subcontractor cost/hours, materials cost, schedule, and list of deliverables. TOs will identify the evaluation criteria from Section B-3 (Determination and Payment of Base and Award Fee) to which the effort under the TO applies. Deliverables will also be specified in the TOs.

Services shall be accomplished through the execution of written TOs. TOs may require the contractor to support efforts that require access to information classified up to and including Top Secret/SCI. The contract will require some, but not all, of the personnel provided by the contractor to have clearances up to that level. The contractor shall include “key PBSC elements” in their proposed task orders as described below:

(a) Performance Work Statement (PWS)
  1. Defines tasks (required results)
  2. Defines performance standards

(b) Quality Assurance Surveillance Plan (QASP)
  1. Defines a standard of metrics and measurements
  2. Defines surveillance methods/measures

(c) Performance requirements summary (PRS)

(Reference CDRL A001, A002, and A003)

2.0 REFERENCE DOCUMENTS

Task Orders will identify any reference documents or GFI/GFM applicable to the order. Reference materials include, but are not limited to the following:

(a) DoD 5000, Federal Acquisition Regulations, and the SPAWAR/PEO-C4ISR Acquisition Program Structure Guide
(b) Business Financial Manager’s Manual
(c) Program Manager’s Handbook
(d) Scheduling Guide
(e) System Engineering Guide
(f) Technology Alignment and Transition Guide and the SPAWAR Contract Procedures and Policy Memoranda
(g) Office of Federal Procurement Policy Letter 91-2 (Service Contracting), dtd Apr 1991
(h) Federal Acquisition Regulation (FAR) Subpart 37.6 (Performance-Based Contracting)
(i) Office of Management and Budgeting (OMB) Memorandum M-01-15 setting PBSC goals for FY 2002 and FY 2005
(j) Government Performance and Results Act of 1993 (GPRA)
(k) DoDD 5200.28
(l) NSTISSP No. 6

(m) NSTISSD No. 501
(n) OMB Circular A-130
(o) DoDD 5200.1
(p) OPNAVINST 5239
(q) SECNAVINST 5239
(r) DODIIS Guide
(s) NAVSO P-5239 Series
(t) OPNAVINST 5530.14B
(u) Information Security Act of 1987
(v) Information Technology Management Reform Act of 1996.

Additional documents may be found on the Navy INFOSEC Website: https://infosec.navy.mil.

3.0 REQUIREMENTS

3.0.1 GENERAL REQUIREMENTS

The government intends to award a performance-based service contract (PBSC) that represents an effort to provide incentives for improved contractor performance standards and to measure the quality of contract performance. Performance-based service contracts structure the acquisition around the purpose of the work to be performed, describing the work in terms of *what is to be accomplished* rather than *how the work is to be* accomplished. The government's focus is on measuring the outcome of the contractor's efforts rather than managing the contractor's efforts. Success is dependent upon use of specific, objective performance measurement criteria and a performance statement of objective that describes the task to be completed rather than giving detailed specifications on how to complete the tasking.

(Reference CDRL A001, A002, and A003)

3.0.2 SPECIAL SECURITY CLEARANCE REQUIREMENTS

A Sensitive Compartmented Information (SCI) security clearance will be required to perform some tasks that contain material that requires special controls for restricted handling within compartmented channels and for which compartmentization is established.

3.0.3 MEDIA CAPABILITIES

The contractor shall have the capability to generate, compile and display various media utilizing software compatible with the government as required by the TOs.

3.1 REQUIREMENTS

3.1.1 BUSINESS PROCESSES

The contractor shall provide technical security expertise and management support to all aspects of IA activities. The contractor shall provide technical expertise to assist the Program Management Office in developing and executing a focused, consistent, and effective IA program compatible with overall IA initiatives and emergent IA technologies.

3.1.2 PLANNING

The contractor shall assist in the development of a master program plan to support IA activities, identifying work breakdown structures, objectives, and approach for IA initiatives. The contractor shall support the identification and development of recommended approaches for the research, development, testing, and evaluation of information systems and equipment needed to satisfy operational IA requirements. The contractor shall assist in developing and recommending changes to the DoN and DoD IA plans. The contractor shall analyze program and other documentation and provide technical support to develop and execute plans for all aspects of IA. The contractor shall support preparation of subordinate project or task management plans as required in order to support the overall IA program to ensure a consistent, compatible, and coordinated IA approach across all functional areas of IA. The contractor shall assist the IA project managers in making technically sound, cost effective, and timely decisions during all aspects of systems acquisition, integration, installation, and support. The contractor shall assist in the development of program/project milestones, schedules, and technical approaches. The contractor shall assist in the development of program/project planning processes and assist in monitoring progress in comparison to agreed plans and schedules. The contractor shall participate and support the preparation for technical interchange meetings/working group meetings and provide technical support to the Program Management Office in the development of IA strategies and functional areas. The contractor shall identify, compare, and recommend standard automated tools to support program management activities, including, but not limited to: planning, scheduling, monitoring, measurement, resource leveling, budgeting, cost control, data collection, issue and action tracking, etc. The contractor shall ensure program management deliverables support the utilization of these selected automated tools. The contractor shall develop and document procedures for program management processes and use of automated tools to support the coordinated cradle-to-grave program management of all IA initiatives. The contractor shall maintain program and project data in a library. The contractor shall assist in the preparation, maintenance, review and delivery of:

(a) Mission Capability Team Matrix
(b) Program Objectives Memorandum
(c) Congressional Justification Book

(d) DIAP Annual Report

(Reference CDRL A001, A002, and A003)

3.1.2.1 PROGRESS TRACKING & EVALUATION

The contractor shall assist in monitoring IA projects through report assessment, program milestone achievement, independent verification and validation (IV&V), compliance with computer resource life cycle management plan (CRLCMP), computer security accreditation plan (CSAP) and other progress measures. The contractor shall provide input for the definition of technological requirements by assessing the state-of-the-art, feasibility of technological alternatives, and the impacts on existing systems. The contractor shall monitor the implementation and results of approved IA activities to support the Program Management Office's implementation of the overall IA program. The contractor shall recommend corrective action or technical options when planned accomplishments or projected IA operational goals are not achieved. The contractor shall attend program reviews, briefings, working groups, tests, and other relevant meetings to communicate and translate joint service security requirements into DoN INFOSEC requirements and provide point papers, trip reports and meeting minutes as required.

(Reference CDRL A001, A002, and A003)

3.1.3 DOCUMENTATION

The contractor shall assist in the development, preparation and maintenance of DoN and DoD policy, procedures, documents, handbooks, newsletters, web sites, and other informational or instructional documentation related to IA and related security areas. Support working groups and forums by developing documentation. The contractor shall prepare draft versions and circulate the drafts for review. The contractor shall collect, organize and review comments by incorporating minor corrections, adjudicating technical comments when appropriate, and identifying and reporting conflicting or substantive comments to the program management office with supporting analysis and recommendations for resolution. The contractor shall maintain an IA library and distribution list and respond to customer requests for IA documentation. The contractor shall monitor changes to policy, programs, and products to identify required changes to published or in-process documentation. The contractor shall prepare documentation changes or updates and circulate them for comment or publication. The contractor shall maintain records of changes and distribute interim and final changes. The contractor shall support PMW C161 proactive communication efforts at all levels to promote IA and security awareness to ensure IA solutions are integrated early into individual command efforts as well as system development and integration efforts. The contractor shall support PMW C161 interface with the vendor community and with other Services and Agencies in order to develop security solutions that ensure PMW C161 IA requirements are visible and known.

The contractor shall prepare input and prepare documentation in draft format, to support IA projects, budgets, and tasking. The contractor shall coordinate document reviews, incorporate comments, and make publications via paper and electronic media. The contractor shall prepare supporting documentation such as spreadsheets, databases, technical reports, and other media as appropriate.

The contractor shall prepare product support documentation to end-users that shall be made available in alternate formats upon request, at no additional charge.
The contractor shall ensure that end-users have access to a description of the accessibility and compatibility features of products in alternate formats or alternate methods upon request, at no additional charge.

The contractor shall ensure that support services for products accommodate the communication needs of end-users with disabilities.

The contractor will assist in the preparation, maintenance, review and delivery of:

(a) Point papers
(b) Reports
(c) Presentations
(d) Analyses
(e) Policy statements
(f) Procedures
(g) Program plans
(h) Meeting minutes
(i) Trip reports
(j) Messages
(k) Correspondence
(l) Briefing inputs

(Reference CDRL A001, A002, and A003)

3.1.4 REQUIREMENTS DEFINTIONS & ANALYSIS

The contractor shall define and recommend approaches for the research, development, testing, evaluation, installation, and support of information systems and equipment to satisfy IA requirements. The contractor shall recommend changes to the DoN and DoD IA goals and initiatives and recommend revisions to IA systems. In addition, the contractor shall develop and present alternatives, scope, cost/schedule analysis and associated risks/benefits for all project phases. The contractor shall identify requirements, cost, schedule and performance criteria to support the Navy's IA goals and initiatives in order to develop and defend existing and future IA budgets, program plans, and policies. Requirements may result from existing IA product lines, integration of IA solutions into legacy systems, integration of IA into developing systems, and/or development of new IA technology and solutions. The contractor shall develop and maintain a current list of communication systems deployed and in development requiring potential IA support. The contractor shall identify and quantify system criticality and risk to the Navy, perform triage and recommend priorities for IA initiatives, and assess all IA technical approaches to ensure consistency with each other. When approaches are determined to be ineffective, inconsistent or incompatible, the contractor shall recommend technical and programmatic changes through either point papers, status reports, program briefings, or other means to provide sufficient information to PMW C161 for evaluation. The contractor shall assist in preparation, maintenance, review and delivery of the following:

(a) Initial Capabilities Document
(b) Capability Development Document
(c) Capability Production Document
(d) Spectrum Certification Compliance
(e) Program planning and guidance documents, such as strategic plans and roadmaps
(f) Analysis, development, review and tracking of acquisition data
(g) Other program documentation

(Reference CDRL A001, A002, and A003).

3.2 THREAT, VULNERABILITY & RISK ANALYSIS

The contractor shall identify and analyze the system concept and identify the operational and functional requirements of new and developing systems in order to develop the system security approach which includes defining security environments, potential threats, vulnerabilities, safeguards, security performance indicators, and risk factors.

(a) The contractor shall identify alternative operational or performance approaches and security measures and compare alternatives by applying decision criteria.
(b) The contractor shall assist in the establishment and maintenance of standard processes and tools for threat, vulnerability, and risk analysis for DoN and DoD systems. The contractor shall develop documentation and training on threat, vulnerability, and risk analysis for users.
(c) The contractor shall conduct threat, vulnerability, and risk analysis of deployed or developing systems. The contractor shall document results of analyses and recommend corrective action, contingencies, lessons learned or other issues.
(d) The contractor shall evaluate threat, vulnerability, and risk analyses conducted on deployed or developing systems. The contractor shall document results of analyses and recommend corrective action, contingencies, and other issues appropriate to each specific analysis.

(Reference CDRL A001, A002, and A003)

3.2.1 STANDARDS

The contractor shall assist in the preparation, maintenance, review and delivery of Operational Requirement Documents (ORD) at a high level and at detailed levels for specified systems. The contractor will provide support to the IA program office for DoD and DoN national/international IA forums (e.g., policy, architecture, standards, and product forums). The contractor shall provide technical support and/or collect data in conjunction with tasking relative to the development and maintenance of IA requirements. The contractor shall provide detailed technical briefs for IA/INFOSEC requirements. The contractor shall assist in the development of standard network security architectures that include voice, video, and data applications. The contractor shall develop and maintain processes and procedures to measure system security effectiveness.

(Reference CDRL A001, A002, and A003)

3.3 ACQUISITION SUPPORT

The contractor shall provide technical support to the Program Management Office in planning and supporting acquisitions. The contractor shall provide support to the program management office to monitor projects with respect to technical objectives, technology utilization, information assurance capabilities, cost, and schedule. This support also includes providing feedback regarding the consistency and compatibility of individual project objectives with overall IA objectives. The contractor shall recommend approaches and detailed requirements to acquire designated IA systems and equipment. The contractor shall provide technical data, analyses, specifications and other input to support technical procurement packages. This includes assisting in the development of Statements of Objectives, equipment specifications, Contract Data Requirements Lists, Security Functional Requirements Specifications, and other procurement related documents. The contractor shall develop and recommend innovative techniques that produce measurable improvements and reduces the acquisition cycle time and life cycle program costs (e.g., commercial-off-the-shelf (COTS) solutions vice non-developmental item (NDI) or in-house development). The contractor shall develop and maintain a system for identifying and tracking procurements or deliverables, including identification and resolution of technical, test, support and management issues. The contractor shall provide representation at acquisition, program management, design, testing, and logistics reviews and provide point papers, trip reports and meeting minutes as required.

(Reference CDRL A001, A002, and A003)

Program Management: The contractor shall assist in development, preparation, analysis, review and delivery of programmatic deliverables that provide data and details that pertain to Information Assurance programs and projects. The deliverables includes but not limited to:

(a) Work Breakdown Structure
(b) POA&M
(c) Analysis, development, review and tracking of acquisition data
(d) Program/project briefings
(e) Project schedules
(f) Cost estimates/models
(g) Command metrics
(h) Cost analyses/monitoring
(i) Cost, technical, and schedule baselines
(j) Development of cost databases
(k) Cost benefit analyses
(l) Development of independent estimates to support ACAT reporting (including TOC)
(m) Cost estimating relationships
(n) Cost models
(o) Earned Value baselines and reports
(p) Risk management
(q) Strategic Planning & Technical Roadmaps
(r) Program/system processes
(s) Prepare and implement operating policies and procedures
(t) Security related measures and controls
(u) Develop Program Protection Plans
(v) Develop Information Assurance Strategies
(w) Information management
(x) Administrative support
(y) Incidental IT support
(z) Organizational training
(aa) Evaluate program management tools

(Reference CDRL A001, A002, A003 and A004)

3.4 INFORMATION ASSURANCE (IA) SYSTEM ENGINEERING

3.4.1 SYSTEM SECURITY ENGINEERING

The contractor shall support system development of IA systems and products. The contractor shall maintain system specifications and prepare updates in the form of Engineering Change Proposals (ECPs) or errata that incorporate comments and changes. The contractor shall ensure that systems engineering decisions are well documented for traceability and audit purposes. The contractor shall investigate operational requirements and perform evaluations and engineering design analyses to ensure that systems being developed or equipment being procured are compatible with feasibility, integration, and interoperability issues. The contractor shall review all relevant regulations, policies, and guidance documentation and coordinate system-related security issues with the Program Management Office and system developers.

The contractor shall assist PMW C161 personnel in providing system security engineering support to developing and fielded systems within SPAWAR and other systems commands. This support involves but is not limited to:

(a) Providing security inputs into system architectures.
(b) Developing C&A plans/procedures.
(c) Recommending IA network security tools to be implemented.
(d) Providing IA technical expertise at interchange meetings/design reviews, and assisting in the development of security policies/procedures.
(e) Providing IA engineering and technical support to Navy IA systems engineering and product analyses.
(f) Investigating system operational requirements and assisting in the development of security functional and performance requirements for new and existing systems.
(g) Developing and maintaining IA system concept specifications on systems and products under development.
(h) Conducting requirements analyses to identify and evaluate proposed changes to IA concept and systems specifications.
(i) Providing IA engineering analysis and technical support for security testing of systems as required during development, installation, and operations to ensure security features are properly functioning.

(Reference CDRL A001, A002, and A003)

3.4.2 SYSTEMS ENGINEERING

The contractor shall support software development and maintenance of IA systems, tools, and products. The contractor shall maintain system specifications and prepare updates in the form of Engineering Change Proposals (ECPs), Software Change Proposals (SCPs) or errata that incorporate comments and changes. The contractor shall ensure that software changes are well documented for traceability and audit purposes. The contractor shall support establishment of a Trusted Software Support Activity (TSSA), including the identification of computer resources needed for supporting the TSSA functions and the development of tools to support the IA enterprise. In addition, the contractor shall:

(a) Develop plans to transition Navy IA products into existing Navy systems and environments, identifying required software interfaces and recommending platforms, porting and software change proposals.
(b) Review and analyze SCPs, software patches, and proposed software implementation/integration support.
(c) Support SSA functions for assigned IA systems, tools, and products, providing pre-SSA support or technical support to assigned SSAs for documentation, support tool development and maintenance.
(d) Provide SSA support for utilization of test/development fixtures, assembler

host operations and maintenance.

(e) Provide Security Systems engineering support for code development and perform software analysis and code modification.

(f) Provide software patches and implementation/integration support for software modules.

(g) Support the SSA in the following tasks: plan, analyze, investigate, design, code, test, integrate, implement, evaluate, support, and deliver software or software changes for IA systems and products in accordance with current security software standards and regulations.

(Reference CDRL A001, A002, and A003)

3.4.3 TEST AND EVALUATION

The contractor shall provide adequate engineering and technical support for Navy laboratory testing of IA systems, software, tools, products and technologies. The contractor shall:

(a) Assist in the development of a Test and Evaluation Master Plan (TEMP) that describes test objectives, critical technical and operational test parameters, and test phases for various efforts.

(b) Assist in documenting test results for conducted tests, including, but not limited to quick-look report, final test report, lessons learned report.

(c) Assist in the analysis and evaluation of test data and reports for tests conducted by other developers or entities and present findings or conclusions.

(d) Provide adequate engineering and technical support for test and test related working groups, meetings, demonstrations, and test events.

(e) Prepare technical papers and briefings to support Navy test responsibilities.

(f) Utilize approved written testing procedures for all software testing. This will include the development of:

(1) Computer Program Test Plan/Software Test Plan

(2) Computer Program Test Specification

(3) Generation of the Computer Program Test Report/Software Test Report.

(Reference CDRL A001, A002, and A003)

3.4.4 TECHNOLOGY DEVELOPMENT

The contractor shall assist PMW C161 in maintaining and enhancing the capability to understand, evaluate, develop, and apply technology to DoN IA and IA problems. This task area includes evaluation of new systems, tools, technology, and Non-Developmental Item (NDI) products; this task also includes the development of:

(a) IA applications

(b) IA tools
(c) IA equipment
(d) IA processes
(e) IA prototypes
(f) IA products/solutions testing, analysis, proof of concept testing, and new technology briefings and demonstrations.

The contractor shall maintain and expand knowledge and expertise in the IA disciplines. The contractor shall explore and investigate evolving systems, threats, issues, products, solutions, technology, tools, operational requirements, and environments that affect the IA arena. The contractor shall provide summary reports, status reports, presentations, and analyses of developing technology areas including the potential affects on DoN/DoD IA. The contractor shall:

(a) Identify, prioritize, and recommend areas of developing technology for more intensive exploration and development by the DoN IA program.
(b) Develop an approach for extended exploration of developing technologies. Approaches may include, but are not limited to: focused research and development, identifying potential applications, utilization in new or existing IA products, developing and conducting tests, feasibility assessment applications or systems, proof of concept scenarios or pilot implementation. Proposed approaches should identify goals, schedules, resources, end products, and other issues.
(c) Provide recommendations for the development, procurement, testing, and operation of IA technologies and security products, systems, tools, literature, etc. to improve IA tools, systems, products and management. The contractor shall make recommendations to support continued evaluation and assessment of new technologies, new applications, and integration with existing systems or environments.
(d) Develop and demonstrate potential IA solutions including, but not limited to, the Programmable Embeddable INFOSEC Product (PEIP), Embeddable INFOSEC Product (EIP) assessing TCP/IP security products and mechanisms, and testing NDI cryptographic and security products.

(Reference CDRL A001, A002, and A003)

3.4.5 IN-SERVICE ENGINEERING ACTIVITY (ISEA) SUPPORT

The contractor shall provide adequate technical support for installation and operational testing of IA systems, devices and tools for both afloat and shore platforms and activities. The contractor shall:

(a) Assist in troubleshooting installation problems and ensuring integration with existing systems and security environment.
(b) Analyze IA system specifications and provide recommendations on

maintenance, training, and support strategy.

(c) Identify sources for support items and maintenance.
(d) Provide interim maintenance and support items for newly developed and deployed systems.
(e) Assist in the development and implementation of integrated logistics support for specified systems.
(f) Identify logistics requirements and prepare recommendations.
(g) Maintain information on installed and planned IA systems, devices, and tools by platform, including detailed information on site specific system versions, planned upgrades, problem areas, corrections, and customized applications.
(h) Conduct site security assessments and integration analyses. The contractor shall provide quick-response reports of security posture to site managers, including analysis of vulnerabilities, conflicts, and recommended solutions.
(i) Provide TEMPEST support, including reviewing TEMPEST Countermeasure Reviews (TCR).
(j) Provide guidance and recommendation for TEMPEST Countermeasures and Program requirements.
(k) Support the Navy Shipboard TEMPEST Inspection Program by and conducting TEMPEST surveys and evaluations on ships, shore installations, and system modifications.

(Reference CDRL A001, A002, and A003)

3.4.6 CUSTOMER SUPPORT

3.4.6.1 HELP DESK

The contractor shall provide adequate technical support to IA customer help desks and provide short-fused technical advice or corrective action. The contractor shall:

(a) Provide 24/7 help desk coverage to the fleet.
(b) Provide solutions for complex Information Security problems and issues.
(c) Provide analysis for IA Help Desk statistics, metrics and problems to identify trends or vulnerabilities requiring additional analyses or resolution.
(d) Provide results of analyses and recommendations as a report.

(Reference CDRL A001, A002, and A003)

3.4.6.2 CERTIFICATION & ACCREDITATION

The contractor shall identify and develop confidentiality, integrity, service availability requirements, and operational constraints for new or existing systems in support of the Designated Approving Authority (DAA). The contractor shall assist in the preparation, maintenance, review and delivery of:

(a) System security certification test and evaluation plans, requirements, and procedures for new and existing information systems.
(b) Security certification and evaluation information is included in the Test and Evaluation Master Plans (TEMP) for programs developing information systems.
(c) Input for and development of draft certification and accreditation documents, including but not limited to:
    (1) Risk assessments of the information system in its anticipated operational environments
    (2) Certification reports
    (3) Recommendations for corrective actions, and other documentation.
(e) Identification and documentation of system threats, vulnerabilities, and existing security measures or safeguards of new or existing systems.
(f) Identification of risk factors such as operational criticality of the system, sensitivity or value of information, associated security environment, and cost of proposed safeguards.
(g) Security certification and accreditation support to fielded systems or systems in development.
(h) Input for development of system Security Authorization Agreements, security accreditation plans, Security Concepts of Operation, system security management plans, system security policies, and security test plans and reports.
(i) Development, maintenance, and definition of IA attributes and metrics for the test and evaluation programs.
(j) Development and maintenance of expertise and tools to apply to the chosen core technologies.

(Reference CDRL A001, A002, and A003)

3.4.6.3 TRAINING

The contractor shall assist in the preparation, maintenance, review and delivery of:

(a) Security training requirements for new or existing systems.
(b) System security training recommendations for the Program Management Office by including proposed training competencies, evaluation requirements, projected target audience, appropriate training tools or training platform (such as computer aided training, video training, classroom training, self-paced, etc.), training sources, estimated costs, schedule, alternatives, or other supporting data.
(c) Existing security training programs and sources to evaluate the effectiveness of meeting established security training competencies.
(d) Issues or deficiencies and recommend alternatives or improvements to existing security training.
(e) New security training programs as required to support a coordinated,

comprehensive DoN and DoD IA training concept.

(Reference CDRL A001, A002, and A003)

3.5 PROGRAM DESCRIPTION

The following paragraphs provide a description of current IA strategic thrusts and product/service areas to be supported under this contract. Since IA is a rapidly evolving arena, these initiatives are intended to be representative and not all-inclusive: Information Assurance IA is the discipline of ensuring the integrity, confidentiality, and availability of our information. Additionally, IA ensures that risks are identified, evaluated, and countered in a reliable and timely manner. IA encompasses the broad range of technology, systems, tools, standards, policy, procedures and products that are used to protect the United States' information resources, detect vulnerabilities, and react to threats regardless of the information medium (i.e. data, voice, video, and imagery). Therefore, IA broadly encompasses information systems security (INFOSEC), TEMPEST, and physical security mechanisms.

3.5.1 NETWORK SECURITY SYSTEMS (NSS)

The NSS program provides for the acquisition of next generation information assurance with computer-network defense in depth security, active security monitoring and security defense management. The NSS product/service area includes a wide range of tasking associated with securing Naval (shore and shipboard) and joint networks. Critical to the NSS product/service area is the definition and standardization of a network security architecture. The NSS product/service area includes the procurement and fielding of Network Security Suites for both ashore activities and afloat platforms. A suite of products consisting of: Host/Embedded Firewalls, High Assurance Guards, Network/Host based Intrusion Detection Systems, Virus Scanning and Virtual Private Networks. NSS also includes the acquisition, integration and implementation of products and services to support Computer Network Defense (CND), Enclave Boundary Protection, Intrusion Detection Systems, Defense Message System (DMS) and other major initiatives, developed by NSA or other In-Line Network Encryptors (INE). The NSS area includes the development and production of the Embeddable INFOSEC Products (EIP), and the assessment of multi-level security (MLS) technologies such as trusted software applications (e.g., databases and operating systems) and Compartmented Mode Workstations (CMWs). The NSS product/service area also covers the tasking associated with planning, executing and deploying intrusion detection capabilities, implementing Defense in Depth (DID) concepts, providing security engineering to promote shore/afloat interoperability, and integrating of next generation NSS products and capabilities. These include Intelligent Agent Security Module, Vulnerability Assessment Tools, Security Asset Accounting Tools and Computer-Network Management Tools. In addition, NSS encompasses the procurement, installation and integration of BLII OCONUS Intrusion Detection System (IDS) management components and the associated infrastructure to enable a fully operational Computer Network Defense (CND) system within the BLII

OCONUS environment.

3.5.2 CRYPTO (READINESS/MODERNIZATION)

Navy Cryptographic (Readiness/Modernization) efforts include the development, acquisition, procurement, integration, test, fielding and sustainment of both legacy and newer cryptographic equipment being developed in support of the Navy's Crypto Modernization Program.

Crypto Modernization devices will include but are not limited to the following: KG-40A, KG-3X Family, Embeddable Information Systems Security (INFOSEC) Product (EIP), Programmable EIP (PEIP), KIV-7 Family, Walburn Family/KIV-19, KG-84, KGV-11, KW-46, IFF and Multi-Functional Crypto Systems (K-09).

Navy Crypto Readiness products provide for the acquisition, procurement, test, integration, and maintenance of crypto devices to support fielded systems and to provide legacy crypto devices to meet urgent fleet shortfalls. Crypto Readiness products provide replacement and sustainment for the retirement of aging, obsolete cryptographic devices that limit the DoN's operational capability and impede progression to network centric architectures and operations. Crypto Readiness devices include but are not limited to the following: KG-175 (TACLANE), KG-75 (FASTLANE), In-line Network Encryptors (INEs), KIV-7, KGV-23, KGV-68B, KIV-6, and KGV-136. Cryptographic assets are essential for assuring the security of the systems and operational effectiveness of the platforms. Crypto Readiness products provide for the security requirements of the following programs: IT-21 (ADNS), BLII (Shore Secure Connectivity to the Piers, and SIPRNET), EHF MDR (which provides TDMA interface), Submarine EHF HDR, SHF installations on CGs and DDGs, Common Data Link, and Shore Cryptologic Support System (SCSS) upgrades. In addition, provide for emerging cryptographic requirements for numerous Fleet Modernization Programs (to include SEAWOLF Class Submarines) and new construction platforms (e.g., Virginia Class Submarines).

3.5.3 INFORMATION ASSURANCE (IA) READINESS

PMW C161 is the IA Readiness Mission Authority. IA Readiness Mission Capability represents the Naval Certification Authority in accordance with OPNAVINST 5239.1B and CNO message traffic. The core effort is to ensure Naval IT systems are designed, installed and operated in compliance with the DoD and DoN system security requirements. IA Readiness performs the duties of the Navy's Information Assurance leader in the areas of certification and accreditation, information assurance dissemination, training, awareness and fleet support through computer network vulnerability assists. In addition, IA Readiness provides technical review/recommendations for information assurance policy. This capability is the primary source for Certified Tempest Technical Authorities for the Navy.

3.5.4 SECURE VOICE

The Secure Voice functional area includes the development of Secure Voice Architecture for shipboard and shore applications. This area encompasses tasks associated with the research, development, procurement, and fielding of secure voice algorithms, devices and systems, including: the procurement of Secure Telephone Equipment (STE) and associated equipment needed to implement the Navy Shipboard Secure Voice Communications Suite (NSSVCS). This area also encompasses activities associated with upgrading secure voice security products, efforts to develop integrated voice/data architectures, and contributions to the overall development and integration of the overarching IO/IA architecture. The STE family of products, FNBDT products, and STU-III family of products are required to satisfy the operational needs for Secure Voice Products. STU-III repairs will need to be extended to provide for minimum secure voice capabilities in the fleet while newer products are fielded, thereby requiring continued services including engineering services, on-site engineering investigations, and assistance for corrections beyond the skill or resource capabilities of the fleet. Other services provided include direct user-customer product maintenance and integrated logistic support activities, user support documentation maintenance, planning for product supply support activity, verification of system operation, and user applications with respect to new voice security products and upgrades. Next generation Secure Voice over IP (SVoIP) developments will continue to evolve the product support for enhanced interoperation with DoD Teleport, Tactical Secure Voice Systems, and advanced Secure Multimedia user capabilities. Additional efforts are to procure and field Secure Voice over IP (SVoIP) terminals and Gateway (SV 21) products. This plan supports the Navy's goal to achieve Network Centric Warfare capabilities and field Secure Voice over IP capabilities.

3.5.5 MULTIPLE SECURITY LEVEL (MSL)/CORSS DOMAIN SOLUTIONS

MSL capability is intended to provide a reconfigurable, enabling architecture, that supports data transfer services at multiple security levels. It will support data exchanges between entities that have varying levels of access control and rules of releasibility, e.g., data transfer from U.S. Secret to NATO Secret or Coalition Secret, etc. The capability will reduce physical footprints, allowing a single workstation/seat to access multiple security networks vice having multiple workstations perform the same function. The architecture development is to support the concept of dynamic coalition membership in addition to treaty alliances such as NATO, US/Korea, Gulf COOP, and AUZCANZUKUS.

MSL Proposed Products/Services include the following:

(a) DII guard
(b) Architecture design and prototype testing and installations
(c) MSL E-Mail and file sharing capabilities

(d) MSL SABI process support and training
(e) Security Engineering for Coalition Interoperability
(f) Web Replication / Collaboration at Sea
(g) Common Operational Picture (COP)
(h) Multi-Level Chat
(i) Coalition Public Key Infrastructure (PKI)
(j) Voice Over IP (VoIP)

3.5.6 KEY MANAGEMENT INFRASTRUCTURE

3.5.6.1 ELECTRONIC KEY MANAGEMENT SYSTEM (EKMS)

The key management product/service area encompasses all activities related to procuring and fielding a fully interoperable, joint, end-to-end, integrated electronic key generation, distribution, and management system. The current predominant focus within the key management product/service area is the development and implementation of the Electronic Key Management System (EKMS) within the DoN. The key management product/service area supports the acquisition, engineering, installation, test, and life cycle support tasks for the Navy-led EKMS Tier 1 System, and the deployment of EKMS Tier 2 (Local Management Device [LMD] and Key Processor [KP]) and EKMS Tier 3 (Data Transfer Device [DTD]) components. The key management product/service area supports select activities designed to investigate and deploy new applications to meet future requirements such as single point keying (SPK) and KMI development and integration efforts.

3.5.6.2 PUBLIC KEY INFRASTRUCTURE (PKI)

PKI provides a foundation for integrated, multi-layered (Defense-in-Depth) protection for network resources and information transfers. It also provides data integrity, authentication, confidentiality and non-repudiation services. Lastly, PKI provides evaluation, testing, and engineering of COTS X.509 CAC-based PKI security components, including application interoperability, procurement, integration and maintenance support. PKI involves deploying a hierarchical infrastructure to support management and control of certificates management infrastructure including hardware, software and management policies to support cryptographic cards, PC cards, and other emerging cryptographic technology. The PKI includes the planning and implementation of Certification Authority Workstations (CAW) and the Organizational Registration Authority Workstations (ORAW). PKI encompasses the broader national effort to track and manage security certificates. The PKI initiative is an effort to provide a range of services to users, including certificate management services, digital signature key management services, confidentiality key, directory services, end-entity initialization services, personal token management services, non-repudiation services and client interface services without requiring the use of FORTEZZA-based products such as the following:

PKI Products/Services Include –

a) Component Authentication Devices (CAD)
b) Token Readers/SIPRNET Token Readers
c) Local Registration Authentication (LRA)
d) Certification Authority Workstations (CAW)

3.5.7 SECURITY SYTEMS ENGINEERING FOR EMERGING FLEET INITIATIVES (SSE)

The System Security Engineering functional area includes the efforts necessary to integrate network security, key management, secure voice, and other architectures into an overarching IA architecture. One initiative is to facilitate the transition and application of new technology to Navy Information Assurance challenges. Emphasis will be placed on providing R&D support for the programs that are identified by the product MCTs as their highest priorities, and emphasis will be placed on increasing the speed of delivery of useful IA capability to Fleet users. This includes the development of a standard security architecture for each discipline/ area, and the coordination with other organizations and functional areas to develop the overarching IA architecture. The System Security Engineering functional area also includes the development of system engineering tools, specific engineering processes, and the implementation of DID concepts in support of the following areas:

(a) Security Analysis & Engineering
(b) Software Engineering
(c) Test and Evaluation
(d) Technology Development

3.5.8 NON-MISSION CAPABILITIES EFFORTS

3.5.8.1 BUSINESS PROCESSES PRODUCT/SERVICE AREA

The Business Processes product/service area is concerned with developing and implementing processes and tools to support the effective operation and management of the enterprise. This area concentrates on financial processes and tools (e.g., financial reporting/execution, POM planning); business management processes and tools (e.g., project management tracking); intra-team communications procedures and mechanisms (e.g., intra-net capability); and data storage, sharing, and retrieval (e.g., common, distributed, accessible database resources).

3.5.8.2 IN-SERVICE ENGINEERING ACTIVITY (ISEA)

The ISEA product/service area includes: the tasking associated with maintaining an INFOSEC In-Service Engineering Activity (ISEA), funding the COMSEC Equipment Repair Program (CERP), and supporting fielded systems. This area also includes the maintenance and manning of the INFOSEC help desk.

3.5.8.3 SOFTWARE SUPPORT ACTIVITY (SSA)

The SSA area includes the delivery of software maintenance activities for IA products and systems. SSA activities are currently focused in the following areas: NKMS Phase I System, Advanced Narrowband Digital Voice Terminal (ANDVT), Common Tier 3 (CT3), and Embeddable INFOSEC Product (EIP).

3.5.8.4 CUSTOMER SERVICE TO OTHER PROGRAMS OF RECORD

The Customer Service product/service area delivers non-product security services to PMW 161 customers. This product/service area provides certification and accreditation (C&A) services and performs security engineering services such as risk assessments. Feedback from Red Teams or other vulnerability assessments are used to target systems that are most at risk. This product/service area covers the delivery of system security engineering services to both Navy and Joint systems being developed such as NMCI, GCCS-M, JMCOMS, FORCENET, DMS, BLII, and SCN initiatives. This area also includes the INFOSEC engineering team support provided to fielded or operational systems in order to improve their security posture. This area is dedicated to providing a high degree of satisfaction to all customers and to providing security education, training, and awareness (ETA) activities to Navy operational and acquisition communities in order to increase the team’s visibility.

3.5.8.5 TECHNOLOGY DEVELOPMENT

The Technology Development functional area includes researching, evaluating, and demonstrating emerging technology for future application as an IA tool or product. Technology development includes developing and demonstrating potential IA solutions, assessing Transmission Control Protocol/Internet Protocol (TCP/IP) security products and mechanisms, and testing non-developmental item (NDI) cryptographic and security products. This area also includes the identification of computer resources needed for supporting the Trusted Software Support Activity (TSSA) functions and the development of tools to support IA initiatives.

3.5.8.6 BIOMETRICS

The Biometrics team is responsible for the development, acquisition, and fielding of biometric security applications that will benefit the Navy both ashore and afloat. The application of biometrics is still in the experimentation phase, only being implemented at selective lab facilities and Navy sites. The team’s goal is to progress from experimentation to permanent installations. This effort is involved in selecting which biometrics are practical and ready for use and which Navy applications will provide the most real-world benefit. The Biometrics team will provide support for operational installations.

A. GLOSSARY

Availability: The goal of ensuring that information and information processing resources both remain readily accessible to their authorized users. Availability of data is data that is in the place, at the time, and in the form needed by the user.
Base Level Information Infrastructure (BLII): Initiative managed by PMW 152 that addresses the upgrade of information technology resources at the outside cable plant of navy bases.
Certificate: Representation of a user's security attributes and privileges, standard format used is X.509.
Certificate Authority Workstation (CAW): Workstation operating with a trusted application used to generate, maintain, and update X.509 certificates.
Certification: Comprehensive evaluation of the technical and non-technical security features of an IS and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified security requirements.
Commercial-Off-The-Shelf (COTS): Refers to those products that were commercially developed and are available for sale, rather than those that were specially developed for and funded by a specific customer (e.g., the U.S. Government).
Confidentiality: Assurance that information is not disclosed to unauthorized entities or processes. Also: The concept of holding sensitive data in confidence, limited to an appropriate set of individuals or organizations. This includes the concept of privacy as defined below.
Cryptographic Logic: Well-defined procedure or sequence of rules or steps used to produce cipher text from plain text, and vice versa, or to produce a key stream, plus delays, alarms, and checks which are essential to effective performance of the cryptographic process.
Data Transfer Device (DTD): Device used to transfer electronic key to cryptographic equipment. DTDs are used at Tier 3 of the EKMS.
Designated Approving Authority (DAA): Official with the authority to formally assume the responsibility for operating an IS or network at an acceptable level of risk.
Electronic Key Management System (EKMS): An initiative comprised of various tiers designed to reinvent the COMSEC material control system (CMCS). Tier 0, the top layer consists of the EKMS Central Facility (CF) that NSA is developing and installing at Ft. Meade and Finksburg, Maryland.
Firmware: Equipment or devices within which computer programming instructions necessary to the performance of the device's discrete functions are electrically embedded in such a manner that they cannot be electrically altered during normal device operations.
FORTEZZA: Family of devices developed under the National Security Agency (NSA) that are used to secure electronic data exchanges. Current implementation is on Type II Personal Computer (PC) card. Contains algorithms for key exchange, encryption, key wrap, hashing, and digital signatures.
Government-Off-The-Shelf (GOTS): Refers to those products that were developed specifically by or for the government, and are currently available for use from a government inventory.

Information Assurance (IA): Information Operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.
Information Operations: Actions taken to affect adversary information and information systems while defending one's own information, and information systems.
Information System: Any telecommunications and/or computer related equipment or interconnected system or subsystems of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice and/or data, and includes software, firmware, and hardware.
Information Systems Security: The protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats.
Information System Security Manager: Person responsible to the activity's DAA who develops, maintains, and directs the implementation of the INFOSEC program within the activity. The ISSM advises the CO on all INFOSEC matters, including identifying the need for additional INFOSEC staff. Serves as the Command's point of contact for all INFOSEC matters and implements the command's INFOSEC program. Previously the ADP Security Officer.
Information System Security Officer (ISSO): Person responsible for ensuring that security is provided for and implemented throughout the life cycle of an information resource. Responsible for implementing system specific security policies in the operational environment. ISSOs are typically responsible for single-user computers (e.g., personal computers and workstations), multi-user computers or departmental Local Area Networks (LANs). The ISSO assists the ISSM in implementing the command's INFOSEC program for an assigned system or area of control. Previously the ADP Systems Security Officer.
Integrity: Ensuring that data has not been modified during transmission
Intelligence: The product resulting from the collection, evaluation, analysis, integration, and interpretation of all available information, which concerns one or more aspects of foreign nations or of areas of foreign operations, and which is immediately or potentially significant to military planning and operations.
Legacy: Refers to systems which are currently deployed on ship and shore stations.
Network: A communications medium and all components attached to that medium whose responsibility is the transference of information. such components may include information systems, packet switches, telecommunications controllers, key distribution centers, and technical control devices.
Network Security Officer (NSO): Individual formally appointed by a designated approving authority to ensure that the provisions of all applicable directives are implemented throughout the life cycle of an information system network.
Privacy: (1) The ability of an individual or organization to control the collection, storage, sharing, and dissemination of personal and organizational information. (2) The

right to insist on adequate security of, and to define authorized users of information or systems. (See the definition for Confidentiality above.)
Public Key: Concept that is part of public/private key implementation, addresses user having both a private and public key. Public key is available to everyone in infrastructure while private key is only held by individual.
Public Key Infrastructure (PKI): Concept referring to the National level (DoD, Federal Government, and Commercial Sector) infrastructure required for the management, distribution, and registration of public keys.
Residual Risk: Portion of risk that remains after security measures have been applied.
Security Safeguards: Protective measures and controls that are prescribed to meet the security requirements specified for an information system.
Sensitive Compartmented Information: All Intelligence Information and material that requires special controls for restricted handling within compartmented channels and for which compartmentization is established.
Sensitive Data: Data that requires protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the data. The term includes unclassified data whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary data, records about individuals requiring protection under the Privacy Act, and data not releasable under the Freedom of Information Act.
Sensitivity: Classification level plus caveats and handling restrictions.
TEMPEST: Short name referring to investigation, study, and control of compromising emanations from telecommunications and automated information systems equipment.